(12) UK Patent Application (19) GB (11) 2 337 908 (13) A

(43) Date of A Publication 01.12.1999

(21) Application No 9905832.3

(22) Date of Filing 12.03.1999

(30) Priority Data
(31) 10063100 (32) 13.03.1998 (33) JP

(71) Applicant(s)
NEC Corporation
(Incorporated in Japan)
7-1 Shiba 5-chome, Minato-ku, Tokyo 108-01, Japan

(72) Inventor(s)
Hiroto Nagai

(74) Agent and/or Address for Service
Mathys & Squire
100 Grays Inn Road, LONDON, WC1X 8AL,
United Kingdom

(51) INT CL[6]
H04L 9/32 // H04Q 7/38

(52) UK CL (Edition Q)
H4P PPEB

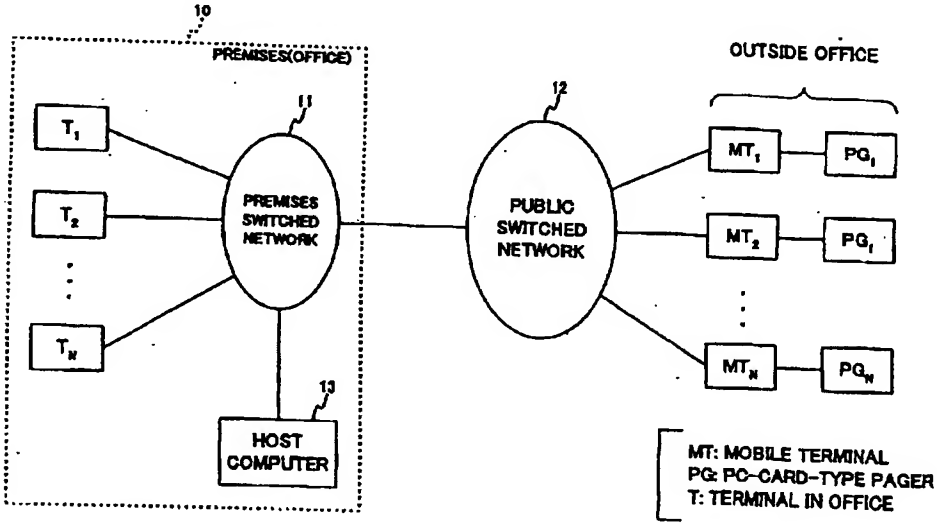
(56) Documents Cited
GB 2300288 A GB 2168831 A GB 2019060 A
EP 0817518 A2 EP 0033833 A2 WO 96/13920 A1

(58) Field of Search
UK CL (Edition Q) G4A AAP, H4L LDSK, H4P PDCSA PPEB PPK
INT CL[6] G06F 1/00, H04L 9/32 12/22, H04Q 7/38

(54) Abstract Title
Accessing a network host computer from outside the network with improved security

(57) An authorised user of a host network 11 such as an office network has a pager in the form of a PC card slotted into a user terminal T_1. To access office network 11 from outside, for example through a public switched network 12, the authorised user is given a one-time password by host computer 13 which is stored in the PC card pager. The PC card pager is then removed from the user terminal T_1 and inserted into a mobile terminal MT_1(for example a notebook computer). Using the mobile terminal the user requests access to the network 11 from outside by sending a username and encrypted authentication information comprising pager ID and one-time password to the host. The user is authenticated and allowed to log in to the network if this information corresponds to information registered in the host computer. Encryption is performed by the PC card pager using a hash function, the authentication information and a random number generator. The mobile terminal may have a wireless or wired connection to the network. A desktop computer may also be used. The one-time password may be transferred to the PC card pager through the paging system.

FIG. 1



GB 2 337 908 A

FIG. 1

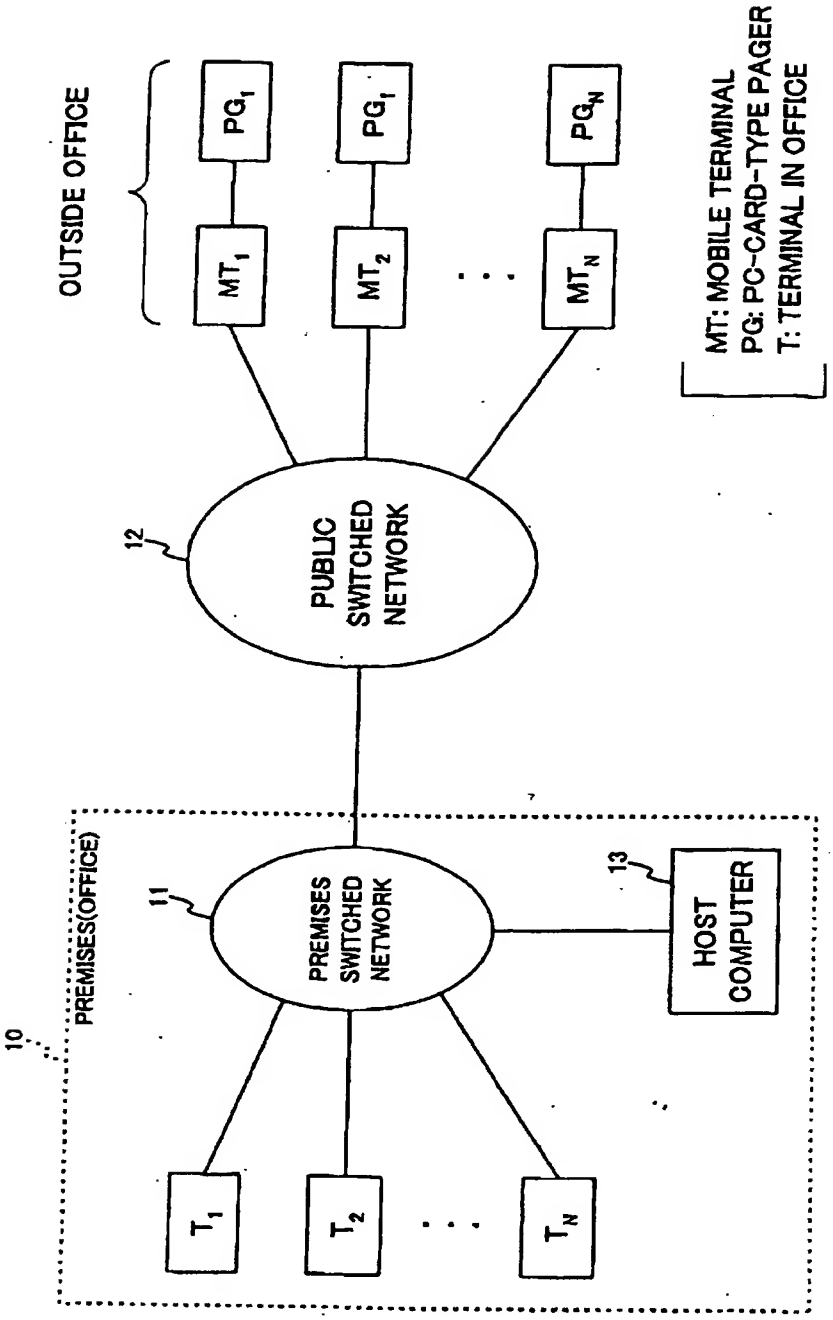

OUTSIDE OFFICE
PG1
PG1
PGN
MT1
MT2
MTN
MT: MOBILE TERMINAL
PG: PC-CARD-TYPE PAGER
T: TERMINAL IN OFFICE
12
PUBLIC SWITCHED NETWORK
10
PREMISES(OFFICE)
11
PREMISES SWITCHED NETWORK
13
HOST COMPUTER
T1
T2
TN

FIG. 2

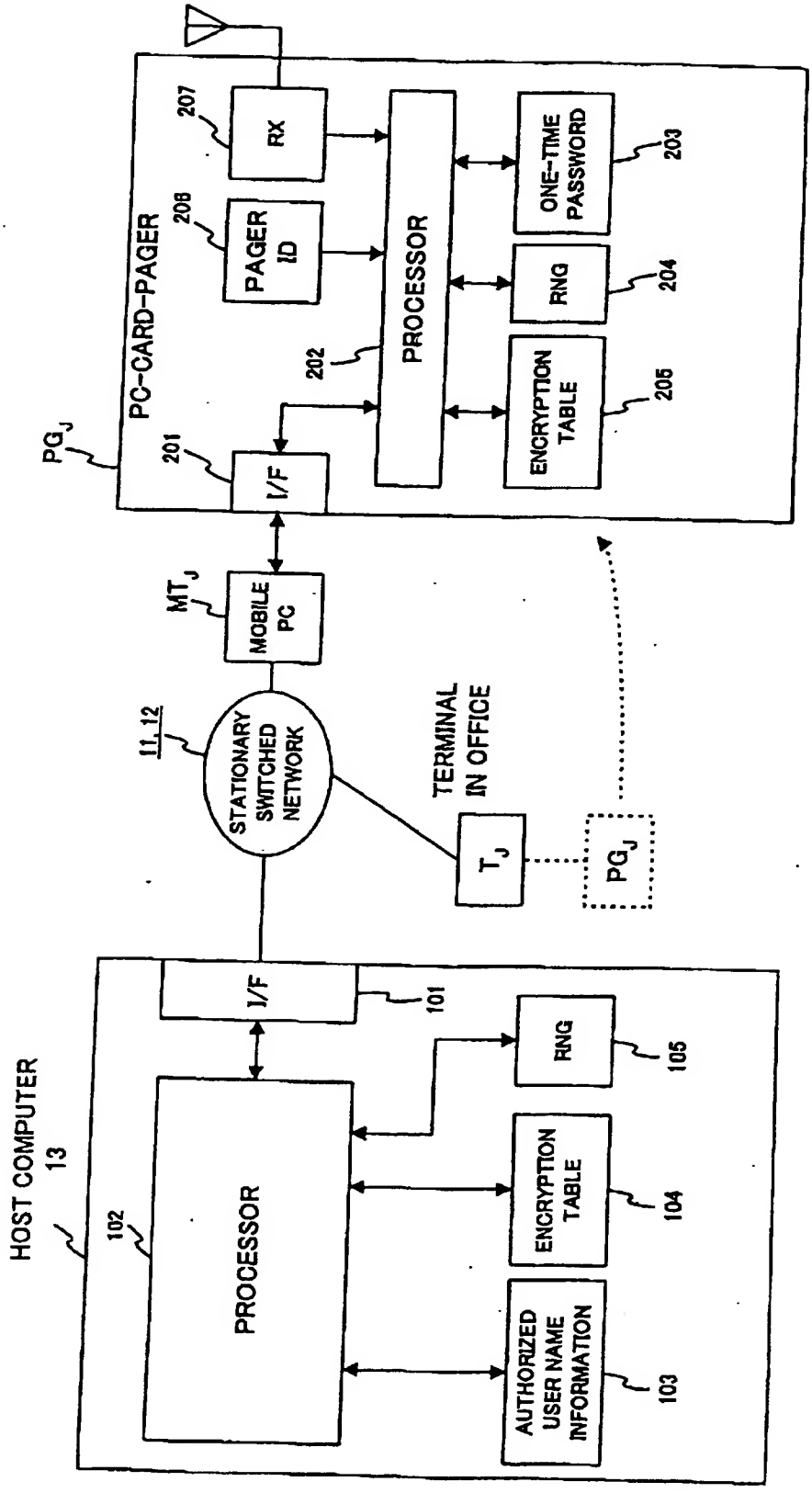

HOST COMPUTER
13
PROCESSOR
102
I/F
101
AUTHORIZED USER NAME INFORMATION
103
ENCRYPTION TABLE
104
RNG
105
STATIONARY SWITCHED NETWORK
11, 12
MOBILE PC
MT_J
I/F
201
PC-CARD-PAGER
PG_J
PROCESSOR
202
RX
207
PAGER ID
208
ONE-TIME PASSWORD
203
RNG
204
ENCRYPTION TABLE
205
TERMINAL IN OFFICE
T_J
PG_J

FIG. 3

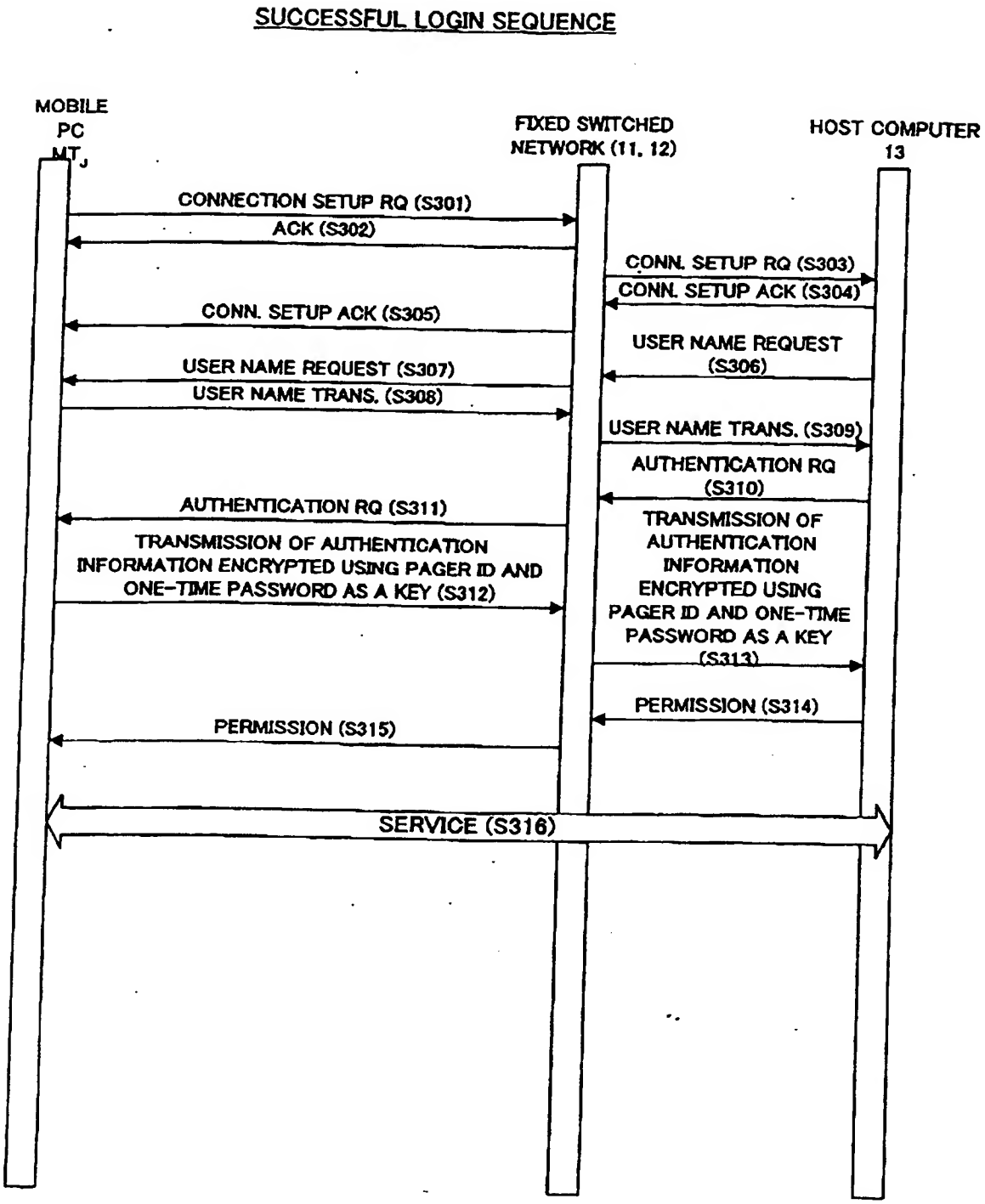

SUCCESSFUL LOGIN SEQUENCE
MOBILE PC MT
FIXED SWITCHED NETWORK (11, 12)
HOST COMPUTER 13
CONNECTION SETUP RQ (S301)
ACK (S302)
CONN. SETUP RQ (S303)
CONN. SETUP ACK (S304)
CONN. SETUP ACK (S305)
USER NAME REQUEST (S306)
USER NAME REQUEST (S307)
USER NAME TRANS. (S308)
USER NAME TRANS. (S309)
AUTHENTICATION RQ (S310)
AUTHENTICATION RQ (S311)
TRANSMISSION OF AUTHENTICATION INFORMATION ENCRYPTED USING PAGER ID AND ONE-TIME PASSWORD AS A KEY (S312)
TRANSMISSION OF AUTHENTICATION INFORMATION ENCRYPTED USING PAGER ID AND ONE-TIME PASSWORD AS A KEY (S313)
PERMISSION (S314)
PERMISSION (S315)
SERVICE (S316)

FIG. 4

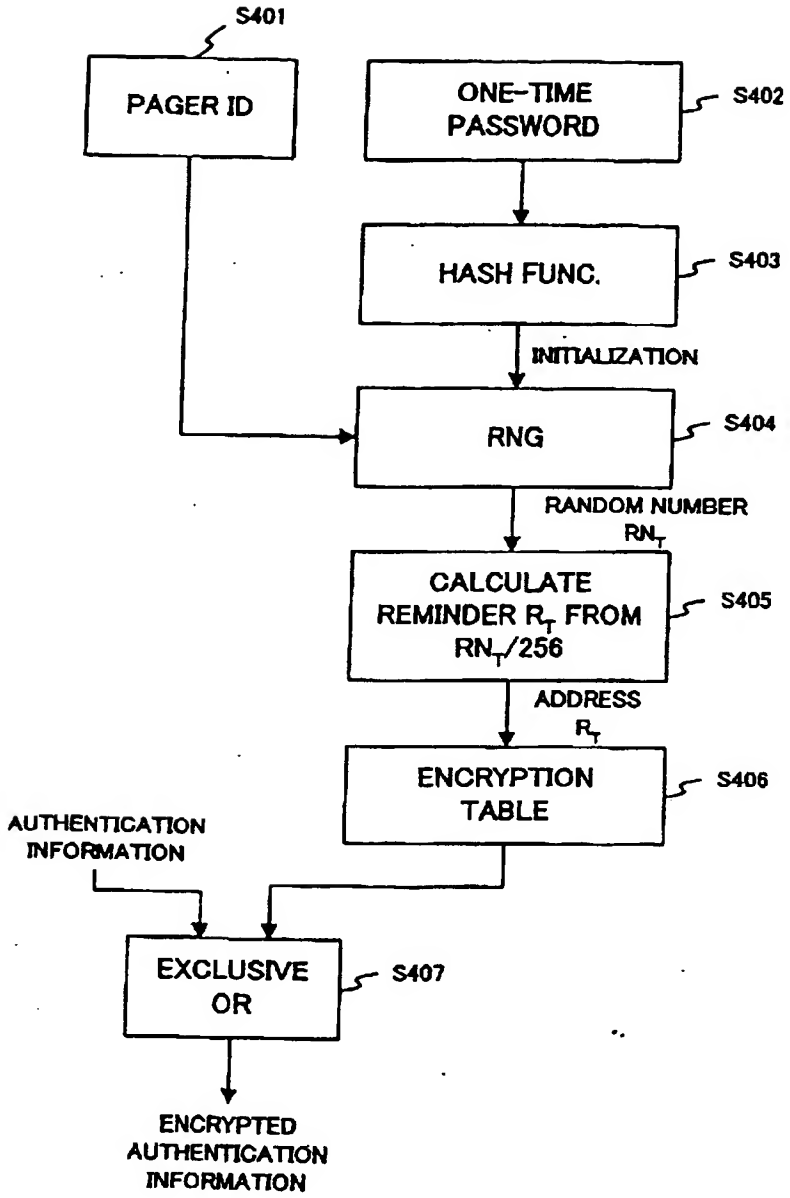

S401
PAGER ID
ONE-TIME PASSWORD
S402
HASH FUNC.
S403
INITIALIZATION
RNG
S404
RANDOM NUMBER
RN_T
CALCULATE REMINDER R_T FROM $RN_T/256$
S405
ADDRESS
R_T
ENCRYPTION TABLE
S406
AUTHENTICATION INFORMATION
EXCLUSIVE OR
S407
ENCRYPTED AUTHENTICATION INFORMATION

FIG. 5

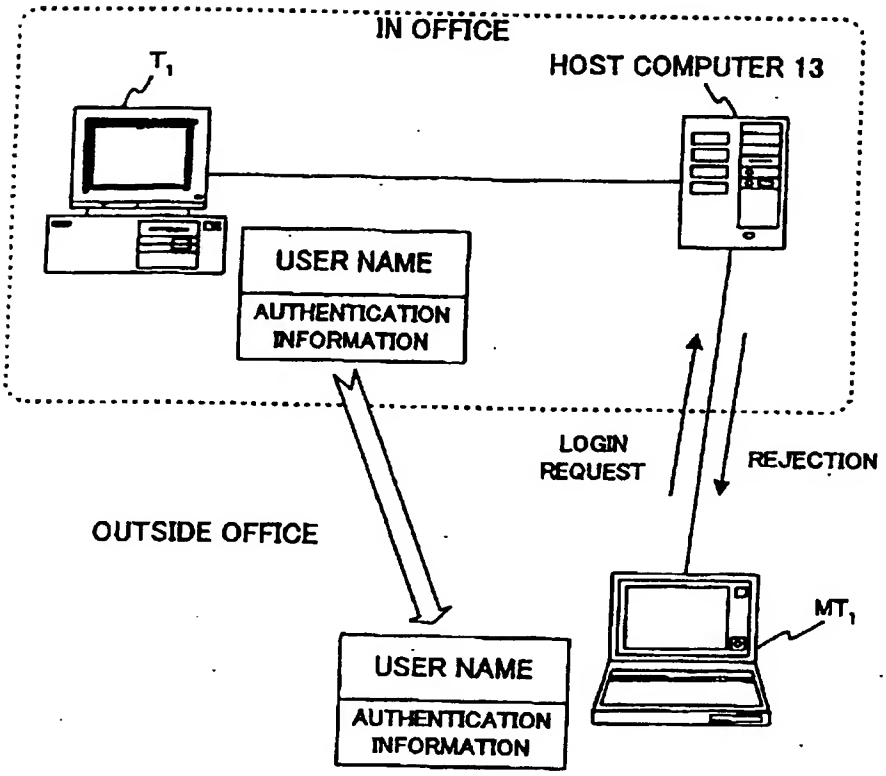

IN OFFICE
T1
HOST COMPUTER 13
USER NAME
AUTHENTICATION INFORMATION
LOGIN REQUEST
REJECTION
OUTSIDE OFFICE
MT1
USER NAME
AUTHENTICATION INFORMATION

FIG. 6

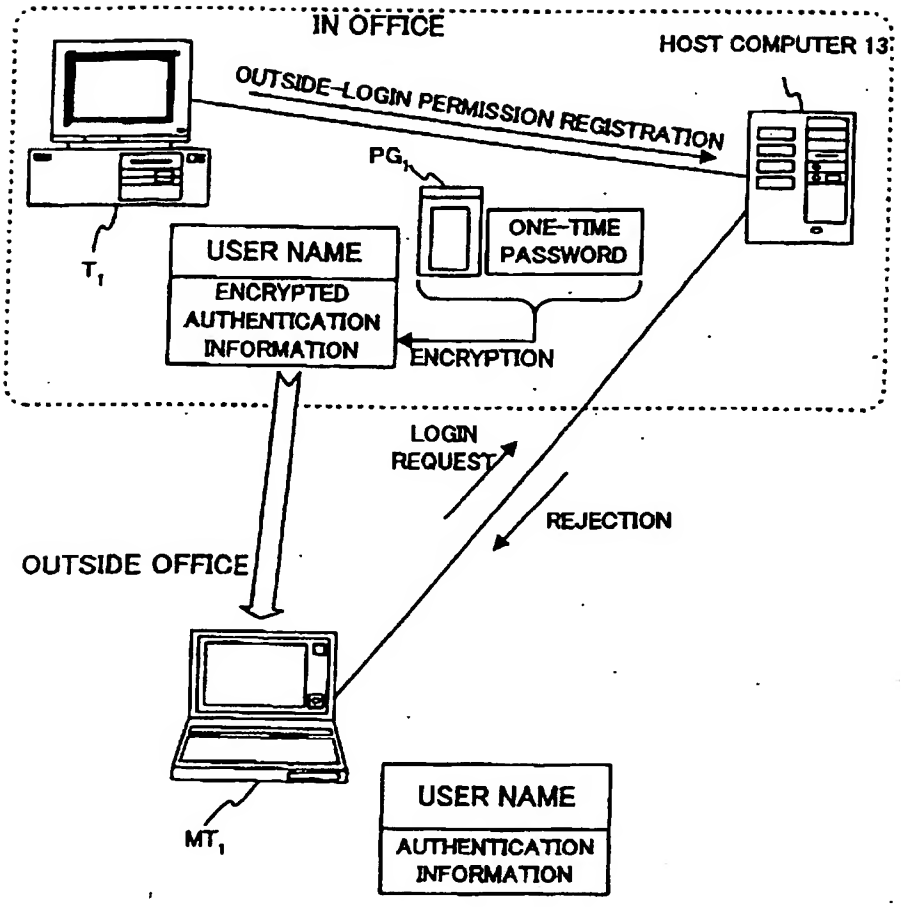
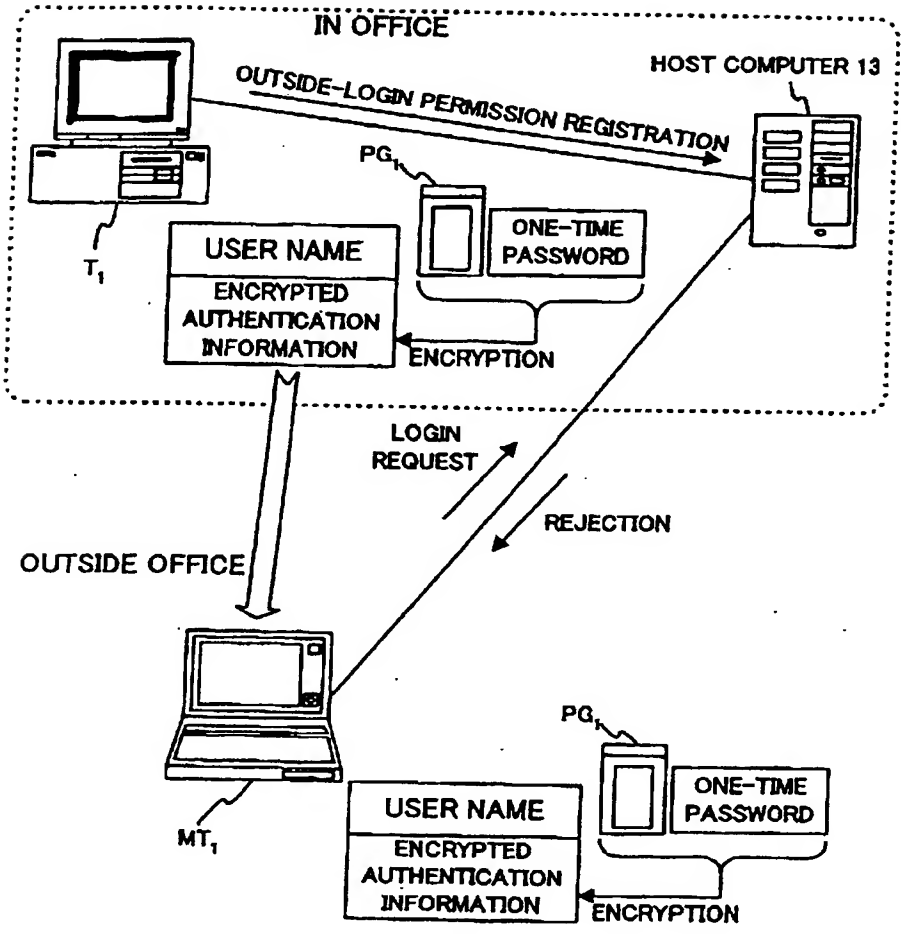

IN OFFICE
HOST COMPUTER 13
OUTSIDE-LOGIN PERMISSION REGISTRATION
PG1
ONE-TIME PASSWORD
T1
USER NAME
ENCRYPTED AUTHENTICATION INFORMATION
ENCRYPTION
LOGIN REQUEST
REJECTION
OUTSIDE OFFICE
MT1
USER NAME
AUTHENTICATION INFORMATION

FIG. 7


IN OFFICE
HOST COMPUTER 13
OUTSIDE-LOGIN PERMISSION REGISTRATION
PG1
ONE-TIME PASSWORD
T1
USER NAME
ENCRYPTED AUTHENTICATION INFORMATION
ENCRYPTION
LOGIN REQUEST
REJECTION
OUTSIDE OFFICE
PG1
ONE-TIME PASSWORD
MT1
USER NAME
ENCRYPTED AUTHENTICATION INFORMATION
ENCRYPTION

2337908

LOGIN PERMISSION METHOD AND SYSTEM

1. Field of the invention

The present invention generally relates to a communications system permitting authorized users to log in to a host computer or server and, in particular, to a login permission method and system from outside to the host computer with improved security.

In a premises network system to which a user can access from outside through a communications line, network security is one of the most important issues. A major focus of network security on computer systems like this is the prevention of system use by unauthorized persons. To protect the system from unauthorized use, the system requires a user to enter a password to verify that the user is authorized to access the network.

According to a conventional security method, a user name and a user's authentication information are registered on the host computer in advance. When a user's mobile terminal has accessed to the host computer through a communications line, the user name is sent to the host computer and, if it matches

the registered user name, then the user's authentication information is also sent to the host computer. In this way, only when both the user name and the user's authentication information match the registered ones, a one-time password is sent from the host computer to the mobile terminal. The mobile terminal is allowed to log in to the host computer using the one-time password.

When an unauthorized person has known the user name and the authentication information of the authorized user, however, the unauthorized person can get the one-time password easily, resulting in compromised security of the network. Further, the conventional technique fails to provide sufficiently rapid connection establishment because the one-time password transmission is performed between the host computer and the mobile terminal during the login process.

An authentication method using secret-key encryption has been proposed in Japanese Patent Unexamined Publication No. 5-327693. A base station transmits random data to a mobile terminal. At the mobile terminal, first and second encrypted authentication signals are produced based on the received random data, a first secret key of the mobile terminal, and a second secret key input by the subscriber, respectively. The encrypted authentication response data is transmitted to the base station.

At the base station, the same encryption process is

performed to produce encrypted check data and matches it with the encrypted authentication response data received from the mobile terminal. If the produced encrypted data matches the received one, the authentication check is affirmative.

In a combination of the conventional one-time password security method and the conventional authentication method using secret-key encryption, pluralities of data exchanges are needed for login between a mobile terminal and a host computer. Therefore, it is very difficult to shorten the time required for login completion.

An object of the present invention is to provide a login permission method and system which can improve network security and efficiently perform a login process at a short time.

According to the present invention, in a host-based network, information required for outside login is previously registered with the host-based network. When an outside login request is received from a terminal through the communications line, it is determined whether user's login information received is validated based on the registered information required for outside login. Only when the user's login information is validated, the terminal is permitted to log in

to the host-based network from outside.

The user's login information is preferably a user name and a user's authentication information, wherein the user's authentication information is encrypted at the terminal and is decrypted at the host-based network according to a predetermined encryption scheme based on the registered information required for outside login. Further preferably, the registered information required for outside login include a unique information uniquely assigned to the terminal, such as an identification number assigned to a selective call receiver or a pager which can be detachably connected to the terminal.

Preferably, the registered information required for outside login further include a one-time password that is temporarily assigned to the terminal by the host-based network when the information required for outside login is registered with the host-based network.

Preferred features of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 is a schematic block diagram showing the configuration of a network system including a login system according to the present invention;

Fig. 2 is a block diagram showing the detailed internal circuits of a host computer and a PC-card pager in an embodiment of a login system according to the present invention;

Fig. 3 is a diagram showing a sequence of a successful login process in an embodiment of a login method according to the present invention;

Fig. 4 is a diagram showing an operation of encryption process in the embodiment of the login method;

Fig. 5 is a schematic diagram showing an operation of the embodiment of the login method when a mobile terminal fails to log in to the host computer;

Fig. 6 is a schematic diagram showing another operation of the embodiment of the login method when a mobile terminal fails to log in to the host computer; and

Fig. 7 is a schematic diagram showing an operation of the embodiment of the login method when a mobile terminal successfully logs in to the host computer.

As shown in Fig. 1, assuming that a network is provided in an office building 10 to provide services to authorized users. The network is composed of a premises switched network 11 which can be connected to a public switched network 12 outside the office, such as the public switched telephone network. Hereinafter, a combination of the premises switched network 11 and the public switched network 12 is called a stationary switched network. The premises switched network 11 is connected to a host computer 13 which can provide services to a plurality of user terminals T_1-T_N installed within the office building 10. For example, an authorized user can log in to the host computer 13 through any user terminal by entering the correct password assigned to the user.

Further, the respective authorized users have PC-card pager PG_1-PG_N and mobile or portable terminals MT_1-MT_N such as notebook computers. A PC-card pager is a PC card having a selective call receiver, or a pager, therein. As described in detail later, a user's PC-card pager stores necessary information including the pager identification number and the encryption table. The PC-card pager is inserted into the PC card slot (PCMCIA slot) of a mobile terminal and thereby the authorized user can log in to the host computer 13 from outside through the public switched network 12. In other words, by connecting the PC-card pager of the authorized user to the

mobile terminal, the user can also log in to the host computer 13 outside the office building 10.

A desktop computer with the communication function and the PC card slot can be also used instead of a mobile terminal MT. That is, the user inserts his/her PC-card pager into the PC card slot of the desktop computer located outside the office and starts the outside login operation as will be described later. Hereinafter, the descriptions will be made in the case of a mobile terminal as an example.

HOST AND PC-CARD PAGER

Referring to Fig. 2, the host computer 13 is connected to the stationary switched network (11, 12) through an interface 101 which may be a modem or a set of digital service unit (DSU) and a terminal adapter (TA). The host computer 13 performs necessary controls including the login control according to the present invention by running control programs on a processor 102.

The host computer 13 further includes a memory 103 for storing authorized user name information, an encryption table 104, and a random number generator (RNG) 105. The authorized user name information includes the user name, the one-time password temporarily assigned to the user, and the pager ID assigned to the PC-card pager PG, to be used by the authorized user. The authorized user name information is registered onto the memory 103 when receiving an outside login permission

request from a user terminal T_J (J = 1, 2, ... ,N) in the office 10. The memory 103, the encryption table 104, and the random number generator 105 are used to decrypt the encrypted authentication information received from the mobile terminal through the stationary switched network. As described later, only users who has been registered in the memory 103 and has sent the correct authentication information encrypted in a predetermined encryption scheme are permitted to log in to the host computer 13.

A PC-card pager PG_J is a PCMCIA card having encryption function and pager function. The PC-card pager PG_J has an interface 201 which is designed to be connected to the PC card slot of a mobile terminal MT_J (here, notebook computer). The PC-card pager PG_J performs the encryption function and the pager function, which may be implemented by programs running on a processor 202.

The PC-card pager PG_J further includes a password memory 203 for storing one-time password, a random number generator (RNG) 204, an encryption table 205, and a pager ID memory 206 storing the pager ID assigned to the PC-card pager PG_J.

The one-time password, as will be described later, is transferred from the host computer 13 to the PC-card pager PG_J and then stored onto the password memory 203 when the PC-card pager PG_J is connected to the user terminal T_J in the office 10 and the user makes the outside login permission request.

The encryption table 205, the random number generator 204, and the pager ID memory 206 are used to encrypt the authentication information of the user. To successfully perform encryption at the PC-card pager PG_j and decryption at the host computer 13, the encryption table 205 and the random number generator 204 of the PC-card pager PG_j are the same as the encryption table 104 and the random number generator 105 of the host computer 13, respectively.

The PC-card pager PG_j further includes a radio receiver 207 which is used to receive a paging or selective calling signal from a radio base station (not shown). As will be described later, the pager function may be used to receive the one-time password from the host computer 13 through a paging system.

The user terminals T_1-T_N each have a PCMCIA slot into which the PC-card pager PG_j is inserted for data communication. More specifically, the pager ID is sent from the PC-card pager PG_j to the host computer 13 and the one-time password is sent from the host computer 13 to the PC-card pager PG_j.

The mobile terminals MT_1-MT_N each have the PCMCIA slot for the PC-card pager and a data communication means for communicating with the host computer 13 through the stationary switched network (11, 12). The data communication means may be a modem or a set of digital service unit (DSU) and a terminal adapter (TA). Alternatively, the data communication means may be a wireless communication means. Further, the mobile

terminals MT_1-MT_N each have a central processing unit (CPU) on which a control program for a PC-card pager may run.

As described before, the present invention is not limited to mobile terminals MT_1-MT_N. A desktop computer with the communication function and the PC card slot can be also used instead of a mobile terminal MT.

LOGIN SEQUENCE

Next, the login procedure will be described in the case where a user having a mobile terminal MT_j and a PC-card pager PG_j therewith logs in to the host computer 13 through the stationary switched network.

When the user intends to log in to the host computer 13 outside the office 10, the user inserts the PC-card pager PG_j of the user's own into the PC card slot of the in-use terminal T_j and then makes the outside login permission request to the host computer 13 through the in-use terminal T_j. When receiving the outside login permission request from the terminal T_j, the host computer 13 reads the pager ID from the PC-card pager PG_j and stores the pager ID and the user name as authorized user name information onto the memory 103. Alternatively, the pager ID may be entered by the user through the keyboard of the terminal T_j.

Next, the host computer 13 informs the user of the one-time password which should be used in the case of outside login through the mobile terminal MT_j. The one-time password

may be displayed on screen of the terminal T_j. Here, assuming that the one-time password is transferred from the host computer 13 to the password memory 203 of the PC-card pager PG_j.

Thereafter, the user logs out and goes out with the mobile terminal MT_j and the PC-card pager PG_j.

Referring to Fig. 3, in the case where the user needs services provided by the host computer 13 from outside, the user inserts the PC-card pager PG_j into the PC card slot of the mobile terminal MT_j and then the mobile terminal MT_j is started making a connection setup request to the stationary switched network (step S301).

If it is possible to establish the requested connection, the stationary switched network sends an acknowledgement (ACK) back to the mobile terminal MT_j and thereby the connection from the mobile terminal MT_j to the stationary switched network is established (step S302). Subsequently, the stationary switched network sends a connection setup request to the host computer 13 (step S303) and, when receiving the connection setup acknowledgement from the host computer 13 (step S304), the connection between the stationary switched network and the host computer 13. Thereafter, the stationary switched network sends a connection setup acknowledgement back to the mobile terminal MT_j and thereby the connection between the mobile terminal MT_j and the host computer 13 is established (step

S305).

When the connection has been established, the host computer 13 sends a user name request for the user name information of the user to the stationary switched network (step S306). When receiving the user name request, the stationary switched network sends the user name request to the mobile terminal MT_j (step S307).

When receiving the user name request from the host computer 13 through the stationary switched network, the user is prompted to enter a user name through the keypad of the mobile terminal MT_j. The user name may be stored in a memory and be read out from the memory in response to the user name request. The user name is sent to the stationary switched network (step S308) and further to the host computer 13 (step S309).

When receiving the user name, the processor 102 of the host computer 13 searches the memory 103 for the received user name. If found, the processor 102 determines that the user name has been registered as an outside login user name and then sends an authentication request to the stationary switched network (step S310) and further to the mobile terminal MT_j (step S311). If not found, the processor 102 determines that the user name has never been registered as an outside login user name and stops the login process to reject the login request.

When receiving the authentication request from the host computer 13, the user is prompted to enter the authentication

information through the keypad of the mobile terminal MT_j. The authentication information may be stored in a memory and be read out from the memory in response to the received authentication request. When the authentication information has been entered, it is transferred to the PC-card pager PG_j. The processor 202 of the PC-card pager PG_j encrypts the authentication information using the pager ID, the one-time password, the encryption table 205, and the random number generator 204. The details of the encryption will be described later.

The encrypted authentication information is sent back to the mobile terminal MT_j and is then transmitted to the stationary switched network (step S312) and further to the host computer 13 (step S313).

At the host computer 13, the encrypted authentication information received from the mobile terminal MT_j is decrypted using the encryption table 104, the random number generator 105 and the authorized user name information in the way similar to the encryption steps performed in the PC-card pager PG_j.

Then, the processor 102 compares the decrypted authentication information with the registered authentication information stored in the memory 103. If the decrypted authentication information matches the registered one, the host computer 13 sends a login permission message to the stationary switched network (step S314) and further to the

mobile terminal MT_j (step S315). In this manner, the user can obtain desired services from the host computer 13 (step S316). Contrarily, If the decrypted authentication information does not match the registered one, the login is rejected.

ENCRYPTION

Referring to Fig. 4, the encryption of the authentication information is performed at the PC-card pager. When the user enters the authentication information, the processor 202 of the PC-card pager PG_j reads the pager ID from the pager ID memory 206 (step S401) and the one-time password from the password memory 203 (step S402). Then, the processor 202 calculates a Hash value H from the one-time password using the Hash function (step S403).

The processor 202 initializes the random number generator 204 according to the Hash value H and then obtains a random number RN_r from the random number generator 104 according to the pager ID (step S404). Further, the processor 202 converts the random number RN_r to a number R_r ranging from 0 to 255 by dividing the random number RN_r by 256 to obtain the reminder R_r thereof (step S405).

Subsequently, the processor 202 reads encryption value from the location of the encryption table 205 which is addressed with the reminder R_r (step S406). Finally, the processor 202 exclusive-ORs the encryption value read from the encryption table 205 and the authentication information entered by the

user to produce encrypted authentication information (step S407). The encrypted authentication information is transmitted to the host computer 13.

When receiving the encrypted authentication information, the decryption steps are performed in the similar way. More specifically, the processor 102 of the host computer 13 reads the pager ID and the one-time password of the authorized user name from the memory 103. Then, the processor 102 calculates a Hash value H from the one-time password using the Hash function and initializes the random number generator 105 according to the Hash value H and then obtains a random number RN_T from the random number generator 105 according to the pager ID. Further, the processor 102 converts the random number RN_T to a number R_T ranging from 0 to 255 by dividing the random number RN_T by 256 to obtain the reminder R_T thereof.

Subsequently, the processor 102 reads encryption value from the location of the encryption table 104 which is addressed with the reminder R_T. Finally, the processor 102 exclusive-ORs the encryption value read from the encryption table 104 and the encrypted authentication information received from the mobile terminal to reproduce the original authentication information. The decrypted authentication information is matched with the registered one.

LOGIN REJECTION AND PERMISSION

Figs. 5 and 6 shows login rejection cases. In the case

shown in Fig. 5, the user is not authorized to log in to the host computer 13 from outside. That is, the user has not been registered onto the memory 103 for outside login permission. Since neither a one-time password nor a pager ID for use in encryption is registered, when the login request of the user is made from outside through the stationary switched network, the host computer determines that the user is an unauthorized person.

In the case shown in Fig. 6, the user has been properly registered onto the memory 103 for outside login permission. Therefore, a one-time password and a pager ID for use in encryption are registered on the host computer 13. In the case where the user does not have the PC-card pager therewith, however, the encryption of the authentication information cannot be performed properly. Therefore, the host computer also determines that the user is an unauthorized person.

Referring to Fig. 7, the user has been properly registered onto the memory 103 for outside login permission and the authentication information is properly encrypted using the pager ID and the one-time password. Therefore, the host computer determines that the user is an authorized person and permits the user to log in to the host computer 13.

As another embodiment of the present invention, the paging system may be used to transfer the one-time password from the host computer 13 to the PC-card pager. More

specifically, the host computer 13 is connected to the paging system and calls up the PC-card pager that the user has. When the PC-card pager has been successfully called, the one-time password is transferred to the PC-card pager through the paging system and is stored onto the password memory 203 of the PC-card pager PG, through the radio receiver 207.

As described above, according to the present invention, only a user who has been authorized to log in to the host computer from outside can log in to the host computer. Especially, the encryption of authentication information is performed based on the pager ID of the PC-card pager of the user's own and the one-time password previously assigned to the user. Therefore, the conditions required for login from outside become more strict, resulting in improved network security.

Since there is no need to send a one-time password from the host computer to the mobile terminal at a login, the login process can be rapidly completed.

Each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features.

Statements in this specification of the "objects of the invention" relate to preferred embodiments of the invention, but not necessarily to all embodiments of the invention falling within the claims.

The description of the invention with reference to the drawings is by way of example only.

The text of the abstract filed herewith is repeated here as part of the specification.

A login permission method improving network security and efficiently performing a login process is disclosed. In a host-based network, information required for outside login is previously registered with the host-based network. When an outside login request is received from a terminal through the communications line, it is determined whether user's login information is validated based on the registered information required for outside login. Only when the user's login information is validated, the terminal is permitted to log in to the host-based network from outside.

Claims:

1. A login permission method to a host-based network from outside through a communications line, characterized by comprising the steps of:

registering information required for outside login with the host-based network;

determining whether user's login information received from a terminal through the communications line is validated based on the registered information required for outside login; and

permitting the terminal to log in to the host-based network from outside only when the user's login information is validated.

2. The login permission method according to claim 1, wherein the user's login information is a user name and a user's authentication information, wherein the user's authentication information is encrypted at the terminal and is decrypted at the host-based network according to a predetermined encryption scheme based on the registered information required for outside login.

3. The login permission method according to claim 2,

wherein the registered information required for outside login include a unique information uniquely assigned to the terminal.

4. The login permission method according to claim 3, wherein the unique information is an identification number assigned to an accessory device incorporated in the terminal.

5. The login permission method according to claim 4, wherein the accessory device is a radio selective call receiver having the identification number previously assigned thereto.

6. The login permission method according to claim 3, wherein the registered information required for outside login further include a one-time password that is temporarily assigned to the terminal by the host-based network when the information required for outside login is registered with the host-based network.

7. The login permission method according to claim 6, wherein the unique information is an identification number assigned to an accessory device incorporated in the terminal.

8. The login permission method according to claim 7, wherein the accessory device is a radio selective call receiver having the identification number previously assigned thereto.

9. A login permission system for permitting a terminal to log in to a host computer of a network from outside through a communications line,

the host computer characterized by comprising:

a registration memory for registering information required for outside login; and

a host processor for determining whether user's login information received from the terminal through the communications line is validated based on the registered information required for outside login and, only when the user's login information is validated, permitting the terminal to log in to the host computer from outside.

10. The login permission system according to claim 9, wherein the user's login information is a user name and a user's authentication information, wherein

the terminal comprises:

a memory storing the registered information required for outside login; and

a encryption processor for encrypting the user's authentication information according to a predetermined encryption scheme based on the registered information required for outside login to produce encrypted user's authentication information,

wherein the host processor decrypts the encrypted user's authentication information received from the terminal according to the predetermined encryption scheme based on the registered information required for outside login to reproduce the user's authentication information.

11. The login permission system according to claim 10, wherein the registered information required for outside login include a unique information uniquely assigned to the terminal.

12. The login permission system according to claim 11, wherein the unique information is an identification number assigned to an accessory device incorporated in the terminal.

13. The login permission system according to claim 12, wherein the accessory device is a radio selective call receiver having the identification number previously assigned thereto.

14. The login permission system according to claim 11, wherein the registered information required for outside login further include a one-time password that is temporarily assigned to the terminal by the host computer when the information required for outside login is registered with the host computer.

15. The login permission system according to claim 14, wherein the unique information is an identification number assigned to an accessory device incorporated in the terminal.

16. The login permission system according to claim 15, wherein the accessory device is a radio selective call receiver having the identification number previously assigned thereto.

17. The login permission system according to any of claims 10 to 16, wherein the terminal comprises:

a computer with a communication function, having a PC card slot therein; and

a PC-card pager which is detachably connected to the PC card slot, the PC-card pager comprising the memory and the encryption processor.

18. A login permission method or login permission system substantially as herein described with reference to the accompanying drawings.

The Patent Office

24

INVESTOR IN PEOPLE

Application No:	GB 9905832.3	**Examiner:**	Gareth Griffiths
Claims searched:	All	**Date of search:**	27 September 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4A (AAP), H4L (LDSK), H4P (PDCSA, PPEB, PPK)

Int Cl (Ed.6): G06F 1/00, H04L 9/32, 12/22, H04Q 7/38

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB2300288 A	(KEW) p.7 line 10 - p.14 line 6	1-5, 9-13
X	GB2168831 A	(STEEBEK SYSTEMS) whole document	1, 9
X	GB2019060 A	(PITNEY BOWES) whole document	1-4, 9-12
X	EP0817518 A2	(AT&T) whole document	1, 2, 9, 10
X	EP0033833 A2	(IBM) page 10 - page 13	1-4, 9-12
X	WO96/13920 A1	(IBM) p19 line 16 - p.21 line 14	1-4, 9-12

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.